Docket No.: 27592-01057-US3
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Hans Wyssen

Application No.: 10/582,831

Confirmation No.: 4997

Filed: April 12, 2007

Art Unit: 2431

For: A METHOD AND SYSTEM FOR VERIFYING DOCUMENTS

Examiner: K. Abrishamkar

REPLY BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

May it please The Honorable Board:

This is Applicants' Reply Brief in response to an Examiner's Answer mailed January 20, 2011. Applicants believe that no fees are required in conjunction with this submission. However, should any fees be due, including if such paper(s) be inadvertently omitted, Applicants authorize such fees to be charged to Deposit Account No. 22-0185, under Order No. 27592-01057-US3, from which the undersigned is authorized to draw.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1208, which begin on the pages as indicated:

I. STATUS OF THE CLAIMS

A. Total Number of Claims in Application

There are 38 claims pending in this application.

B. Current Status of Claims

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-38
4. Claims allowed: None
5. Claims rejected: 1-38

C. Claims on Appeal

The claims on appeal are 1-38.

II. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-38 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,587,945 to Pasieka (hereinafter "Pasieka") in view of U.S. Patent No. 7,295,677 to Simpson et al. (hereinafter "Simpson").

III. ARGUMENT

Applicants maintain the arguments as presented in the Appeal Brief filed on November 8, 2010. Applicants would also like to address some statements made in the Examiner's Answer mailed on January 20, 2011.

Applicants initially note that the Examiner's Answer continues to lack any teachings or suggestions of a "separately derived electronic displayable verification information corresponding to the electronic displayable verifiable provenance" as recited in representative independent Claim 1, and as discussed in Applicants' Appeal Brief. *Appeal Brief, pgs. 14-16.* The Examiner's Answer attempts to rebut Applicants' assertion to this end by arguing that Pasieka's teaching of an image fingerprint related to a document teaches such a limitation. *Examiner's Answer, pgs. 18-19.* However, the Examiner's reliance on Pasieka's image fingerprint is without merit. For example, Pasieka recites:

> The server combines the imager ID (or author ID) and image sequence number with the image to produce an image record ... The server hashes the image record using a one-way hash to produce an image fingerprint. The author ID (or scanner ID) ... [is] included in the image record to provide evidence of the origin of the ***image***. (Emphasis added). *Pasieka, col. 4, lines 33-36; col. 5, lines 4-6.*

From this passage of Pasieka, Pasieka teaches information corresponding to the origin of the ***entire image***, rather than verification information corresponding to the electronic displayable verifiable provenance contained within the image. (Emphasis added).

The Examiner's Answer also continues to lack any teachings or suggestions of "the verification information ... displayed on the image data" as recited in representative independent Claim 1. The Examiner's Answer argues that Simpson teaches this limitation. More particularly, the Examiner's Answer argues that "Simpson discloses a visible watermark which is placed on an image which provides authentication information about the user on it." *Examiner's Answer, pg. 4.* This argument is without merit. Even assuming, *arguendo*, the Simpson watermark equates to authentication information, Simpson still fails to teach verification information corresponding to the provenance of the image. For example, Simpson teaches systems and methods for adding a visible watermark. *Simpson, Abstract.* Simpson also teaches that a watermark marks the primary image as the property of the owner (or marks the image in some other way, such as indicating that the primary image is a "draft" image). *Simpson, col. 5, ll. 8-12.* However, nowhere does Simpson teach any authentication information corresponding to an electronic displayable verifiable provenance contained within the image.

Finally, although Applicants have presented arguments relating to the individual references, these arguments are directed to showing the flaws that exist even when the teachings of the references are combined. This is clear from the fact that Applicants' Appeal Brief includes mention of Simpson when discussing Pasieka and vice versa. In other words, Applicants have addressed, not only the individual references, but their combination, as well, by demonstrating that neither cures the deficiencies of the other and that one could not combine them to obtain all of the elements found in the claims.

Therefore, Applicants continue to maintain that all claims on appeal are allowable over the cited references.

Dated: March 18, 2011

Respectfully submitted,
Electronic signature: /Jefferson Cheatham/
Jefferson Cheatham
Registration No.: 67,621
CONNOLLY BOVE LODGE & HUTZ LLP
1007 N. Orange Street
Wilmington, DE 19801
(302) 658-9141
(302) 658-6514 (Fax)
Attorney for Applicants

APPENDIX A - CLAIMS

1. A computer system, comprising:

a memory configured to store electronic image data corresponding to an original document having an electronic displayable verifiable provenance, and separately derived electronic displayable verification information corresponding to the provenance of at least part of the original document, and

an output configured to provide said image data and said verification information for display by the user to authenticate the original document,

wherein the verification information is displayed on the image data.

2. A computer system according to Claim 1 wherein the image data has been obtained from an authenticated source, and the verification information includes data corresponding to the provenance of the authenticated source.

3. A computer system according to Claim 1 wherein data is fed to and from the memory under the control of a repository.

4. A computer system according to Claim 3 wherein the verification information comprises data concerning the provenance that has been subjected to authentication by the repository, and the verification information being configured to signal to the user that the repository provides such authentication.

5. A computer system according to Claim 2 wherein data stored in the memory cannot be altered by users.

6. A computer system according to Claim 3 including apparatus to receive the image data from a remote location.

7. A computer system according to Claim 1 including a scanner for scanning an original document to produce said image data.

8. A computer system according to Claim 1 including a repository agent including apparatus operable to send image data corresponding to an original image to the repository.

9. A computer system according to Claim 8 wherein the repository agent is operable to send the image data together with source authentication information to indicate to the repository that the image data has been sent from the agent.

10. A computer system according to Claim 1 wherein the verification information comprises predetermined accreditation indicia to be viewed by a user concurrently with the image data for authenticating individual parts of the original document.

11. A computer system according to Claim 1 wherein the verification information comprises accreditation data to be viewed by a user in a separate field associated with the image data for authenticating the original document.

12. A computer system according to Claim 1 wherein the image data and the verification information are stored in a common electronic file.

13. A computer system according to Claim 12 wherein the file is a PDF file.

14. A computer system according to Claim 1 including a server providing said memory and operable to host a website at which said image data and verification information is viewable by a user to authenticate the original document.

15. A computer system according to Claim 1 wherein said output is connected to the Internet.

16. A computer system according to Claim 1 wherein said image data and verification information in the memory is password protected so that the user can only gain access thereto by use of the password.

17. A computer system according to Claim 1 wherein the image data and the verification information corresponding to the original document when stored in the memory collectively has an individual addressable identity.

18. A method of operating a computer system according to Claim 1 to provide said image data and said verification information for display by the user to authenticate the original document.

19. A method of displaying a document for authentication, comprising:

creating electronic image data corresponding to an original document having an electronic displayable verifiable provenance;

providing electronic, displayable verification information corresponding to the provenance of at least part of the original document; and

displaying the image data and the verification information, to permit a user to authenticate the document,

wherein the verification information is displayed on the image data.

20. A method according to Claim 19 including receiving the image data from an authenticated source, storing the image data for display, and creating the verification information for the received image, wherein the verification information includes data corresponding to the provenance of the authenticated source.

21. A method according to Claim 19 including authenticating the source of the image data.

22. A method according to Claim 18 including feeding the image data and the verification information to a memory under the control of a repository for display to users wishing to authenticate the original document.

23. A method according to Claim 22 wherein only the repository can change the data in the memory.

24. A method according to Claim 22 wherein the verification information comprises data concerning the provenance that has been authenticated by the repository.

25. A method according to Claim 24 wherein the repository communicates with the source of the image data to determine the provenance thereof and to develop said verification information.

26. A method according to Claim 22 including feeding the image data to the repository from a remote location.

27. A method according to Claim 22 including sending said image data corresponding to an original image from a repository agent to the repository.

28. A method according to Claim 26 including sending the image data together with source authentication information to indicate to the repository that the image data has been sent from the repository agent.

29. A method according to Claim 18 including configuring the verification information to include predetermined accreditation indicia viewable concurrently with the image data for authenticating individual parts of the original document by a user that authenticates the document.

30. A method according to Claim 18 including configuring the verification information to comprise accreditation data to be viewable by a user in a separate field associated with the image data for authenticating the original document.

31. A method according to Claim 18 including storing the image data and the verification information are stored in a common electronic file.

32. A method according to Claim 18 including storing the image data and the verification information are stored in a common electronic PDF file.

33. A method according to Claim 18 including hosting a website at which said image data and verification information is viewable by a user to authenticate the original document.

34. A method according to Claim 18 including authenticating the original document by viewing said electronic image data and the corresponding verification information.

35. A method according to Claim 18 wherein said image data and verification information is password protected so that a user can only gain access thereto by use of the password, and including supplying the password to a user to permit the user to authenticate the original document.

36. A method according to Claim 18 wherein the image data and the verification information corresponding to the original document collectively have an individual addressable identity and including supplying the individual addressable identity to a user to permit the user to access the data and information for authenticating the original document.

37. A method according to Claim 35 including supplying a hyperlink to the user.

38. A computer system comprising:

a unit for processing an electrical signal for displaying a document for authentication to be received by a client computer operated by a user who wishes to authenticate the document, wherein the electronic signal comprises:

electronic image data corresponding to an original document having an electronic displayable verifiable provenance; and

electronic, displayable verification information corresponding to the provenance of at least part of the original document,

wherein the verification information is displayed on the image data.